La protection des données et le contrôle de l'utilisation de moyens de communications électroniques dans la relation de travail

Rosier, Karen

Published in:
Défis du droit à la protection à la vie privée

Publication date:
2008

Document Version
le PDF de l'éditeur

LA PROTECTION DES DONNÉES ET LE CONTRÔLE DE L'UTILISATION DE MOYENS DE COMMUNICATIONS ÉLECTRONIQUES DANS LA RELATION DE TRAVAIL : QUEL CADRE NORMATIF EUROPÉEN ?

Karen Rosier

Chercheuse au CRID (Centre de Recherches Informatique et Droit) à Namur
Avocate au barreau de Bruxelles (Cabinet d'avocats Stibbe)

Sommaire : I. Introduction. II. Cadre normatif. III. Règles émanant de la directive 95/46/CE. III.1. L'usage du courrier électronique par les travailleurs : qui est le responsable de ces traitements ? III.2. Le contrôle en tant que traitement de données à caractère personnel. III.2.1. Principe de licéité. III.2.2. Principe de transparence. III.2.3. Principe de finalité. III.2.4. Principe de nécessité. III.2.5. Principe de légitimité. III.2.6. Principe de proportionnalité. III.3. Le contrôle et les données sensibles. IV. Règles émanant de la directive 2002/58/CE. IV.1. Principe de l'interdiction de la surveillance et de l'interception de communications électroniques. IV.1.1. Portée du paragraphe 1 de l'article 5. IV.1.1.1. Les informations protégées. IV.1.1.2. Les traitements pris en considération. IV.1.1.3. Cadre technique. IV.1.2. Principe. IV.1.3. Conclusion. IV. 2. Accès aux données de communications. V. Conclusion.

Résumé : L'usage de plus en plus répandu du courrier électronique et de l'Internet ainsi que la mise à disposition de téléphones mobiles offrent l'occasion d'un contrôle accru des travailleurs- souvent à l'insu de ces derniers- et rendent plus diffuse la séparation entre vie privée et vie professionnelle. Cette évolution réveille ou suscite d'intéressantes questions dans le domaine de la protection des données à caractère personnel. Elle crée notamment de nouveaux défis en matière de conciliation de l'intérêt des travailleurs à voir leurs droits fondamentaux respectés, en particulier leur droit à la vie privée, d'une part, et les intérêts légitimes qu'un employeur peut avoir de contrôler ses travailleurs.

Au niveau européen, le contrôle et la surveillance de l'usage de ces outils devront, lorsqu'ils sont effectués au moyen de traitements automatisés en tout ou en partie sur des données à caractère personnel, respecter les principes définis par la directive 95/46/CE. L'application de certains de ces principes dans ce contexte ne va pas sans poser des difficultés. La prise de connaissance d'une communication

électronique ou même des données de transmission soulève également l'épineuse question de la confidentialité des communications prévue à l'article 5 de la directive 2002/58/CE ainsi que du traitement des données relatives aux communications électroniques. La combinaison de ces dispositions limite fortement les possibilités de contrôle et de surveillance du travailleur par l'employeur. La Commission européenne qui s'est penchée notamment sur cette problématique envisage d'ailleurs d'introduire de nouveaux principes pour encadrer ces activités de contrôle au sein d'une proposition de directive spécifique au traitement des données à caractère personnel dans la relation de travail.

1. INTRODUCTION

Il n'est plus contesté aujourd'hui que la protection de la vie privée ne s'arrête pas dès franchie la porte de l'entreprise. En effet, tant la jurisprudence de la Cour européenne des droits de l'homme que la directive 95/46/CE consacrent une protection de la vie privée dans le monde du travail.

Dans son arrêt Niemietz du16 décembre 1992, la Cour européenne des droits de l'homme affirmait qu'il serait trop restrictif de limiter la notion de vie privée à un « cercle intime » et indiquait que le respect de la vie privée doit également englober, dans une certaine mesure, le droit pour l'individu de nouer et de développer des relations avec ses semblables (1).

Face à cette protection de la vie privée dont il convient de tenir compte, l'employeur a également un intérêt certain à contrôler l'usage des outils de travail mis à la disposition de ses travailleurs. Dans une certaine mesure, il se doit même de maintenir un contrôle dès lors notamment que sa responsabilité vis-à-vis de tiers ou de ses travailleurs pourrait se voir engagée. Ainsi en est-il par exemple de l'obligation de l'employeur de faire respecter les bonnes mœurs et de prendre des mesures ou sanctions contre les comportements déplacés de ses travailleurs vis-à-vis de leurs collègues de travail. On pense également à l'exemple de propos diffamatoires ou racistes diffusés par le biais de la messagerie de l'employeur par des travailleurs indélicats.

Le contrôle peut prendre différents visages selon qu'il est ponctuel (par exemple pour répondre à des soupçons précis qu'un employeur aurait face à ses travailleurs) ou continu (surveillance pour assurer le bon fonctionnement d'un système informatique). Il peut également être général et viser l'ensemble ou une catégorie de travailleurs ou ne cibler qu'un travailleur, pour mettre au clair un comportement en particulier.

(1) Affaire *Niemietz c. Allemagne*, Cour eur. D.H., 23 novembre 1992, Séries A N° 251/B, §29.

Notre propos n'est pas de procéder à un examen exhaustif de cette problématique mais plutôt de mettre en lumière quelques questions épineuses qui se posent lorsqu'il s'agit de confronter les règles émanant des directives européennes relatives au traitement de données à caractère personnel avec la réalité du contrôle et la surveillance de l'usage du courrier électronique, de l'Internet et du téléphone.

Dans un premier temps, nous ferons le point sur les directives applicables à la matière. Sans revenir sur le contenu de toutes leurs dispositions, nous nous interrogerons sur le lien qui les unit et la manière de concilier l'application concurrente de ces deux directives (Section 2). Nous envisagerons ensuite certaines des règles qui émanent de chacune d'elles et qui ont un impact sur la surveillance et le contrôle de l'usage du courrier électronique, de l'Internet et du téléphone et nous nous emploierons à en cerner les implications dans ce contexte particulier (Sections 3 et 4). Nous conclurons enfin par une synthèse de ces exigences et par une évaluation de leur adéquation et application dans le cadre de ces traitements de contrôle (Section 5).

II. Cadre normatif

Le législateur européen n'a, jusqu'à présent, pas adopté de directive européenne spécifique aux traitements de données dans le cadre de la relation de travail. Une réflexion est cependant en cours concernant l'opportunité d'adopter une directive spécifique au traitement de données à caractère personnel dans le contexte professionnel. C'est dans ce cadre que le Groupe de l'article 29 a rendu un avis sur la question (2) et que la Commission a lancé une procédure de consultation des partenaires sociaux (3).

Le siège de la matière est donc le droit commun de celle-ci, à savoir la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la circulation des données (4) et la directive 2002/58/CE relative à la vie privée et aux communications électroniques du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère

(2) Avis 8/2001, du 13 septembre 2001 sur le traitement de données à caractère personnel dans le contexte professionnel, 5062/01, WP 48, p. 4.

(3) La Commission a publié un document intitulé « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultdataprot_fr.pdf.

(4) *J.O.C.E.*, n° L 281, 23 novembre 1995, p. 0031-0050.

personnel et la protection de la vie privée dans le secteur des communications électroniques (5).

La législation relative à la protection des données qui cultive l'objectif d'assurer une protection de la vie privée des individus s'applique indépendamment du fait que des données traitées se rapportent à un contexte professionnel ou à la sphère privée de la vie de la personne concernée par celles-ci (6). Les conditions et restrictions posées aux traitements de données à caractère personnel par la directive 95/46/CE s'appliquent donc pleinement dans le contexte du travail, en ce compris aux traitements mis en oeuvre par l'employeur sur des données relatives à ses travailleurs. De même, les dispositions de la directive 2002/58/CE protègent les abonnés et utilisateurs indépendamment du contexte dans lequel il est fait usage des services de communications électroniques et de réseaux de communications électroniques. Le secret des communications en particulier est également garanti dans le contexte de la relation de travail.

Quant à l'interaction qui existe entre les deux directives, la directive 2002/58/CE contient une précision importante en son considérant 10 à cet égard : la directive 95/46/CE est applicable au secteur des communications électroniques, et ce tant dans le secteur public que dans le secteur privé. Elle définit, en outre, un rapport de subsidiarité entre les deux directives: pour tout ce qui n'est pas expressément réglé par la directive 2002/58/CE, il convient de se référer aux dispositions de la directive 95/46/CE.

Les liens entre les deux directives ne sont cependant pas purement ceux d'une directive générale et d'une directive particulière appliquant strictement les principes de la première au secteur des communications électroniques. En effet, la directive 2002/58/CE ne se réfère que très peu aux concepts clés de la directive 95/46/CE, tels la notion de « responsable de traitement » ou de « légitimité » du traitement, et se présente davantage comme une régulation parallèle qui s'applique, la plupart du temps, cumulativement aux règles relatives aux traitements de données à caractère personnel définis dans cette deuxième directive. Ceci peut être source de certaines difficultés, notamment lorsqu'il ne ressort pas clairement du texte des dispositions de la directive 2002/58/CE qu'elles dérogent à la directive 95/46/CE.

(5) *J.O.C.E.*, n° L 20, 31 juillet 2002, p. 0037-0047.

(6) Le Groupe de l'article 29 l'a d'ailleurs rappelé dans son avis 8/2001, *op.cit.*, p. 3.

III. Règles émanant de la directive 95/46/CE

III.1. L'usage du courrier électronique par les travailleurs : qui est le responsable de ces traitements ?

Les dispositions de la directive 95/46/CE ont déjà fait l'objet de nombreux commentaires. Il nous semble toutefois qu'on est loin d'avoir mesuré toutes les implications que ce texte peut avoir. L'une d'elles concerne, nous semble-t-il, son application au courrier électronique. En effet, il est indéniable que la rédaction, l'enregistrement ou encore l'envoi d'un courrier électronique contenant des données à caractère personnel constitue bel et bien un traitement de données à caractère personnel au sens de l'article 2, b de la directive. Il s'agit d'opérations effectuées à l'aide de procédés automatisés sur des données à caractère personnel. Cette conclusion est soutenue d'ailleurs par l'arrêt Lindqvist de la Cour européenne des droits de l'homme au terme duquel la simple mention d'une donnée à caractère personnel sur un site Internet emporte application de la directive (7). Il n'est donc nul besoin d'un quelconque ordonnancement spécifique des données pour tomber sous le coup de l'application de la directive 95/46/CE.

Ceci nous amène à nous interroger sur l'identité du responsable des traitements relatifs à la correspondance par courrier électronique effectuée à partir de la boîte professionnelle du travailleur. Aux termes de l'article 2, d de la directive 95/46/CE, le « responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ».

Dès lors que l'outil qu'est le courrier électronique est mis à la disposition des travailleurs par l'employeur et qu'il est utilisé dans le cadre des activités professionnelles du travailleur, on considérera sans difficulté que l'employeur est bien le responsable de ces traitements. En effet, dans ce cas, l'utilisation du courrier électronique interviendra dans le cadre d'un traitement, entendu comme un ensemble d'opérations appliquées à des données à caractère personnel, décidé par l'employeur (telles la gestion de la clientèle, la gestion des salaires, etc.). Dès lors que la correspondance par courrier électronique est envisagée comme une tâche accomplie par le travailleur dans le cadre de la mise en œuvre d'un traitement décidé par l'employeur, c'est ce der-

(7) Arrêt de la C.J.C.E., 101/01, *Bodil Lindqvist*, 6 novembre 2003, disponible sur le site http://curia.eu.int.

nier qui sera considéré comme responsable de traitement. Ses travailleurs n'auront pas même la qualité de sous-traitants dès lors qu'ils agissent sous son autorité.

Par contre, lorsqu'il s'agit d'un usage par le travailleur du courrier électronique à des fins autres que professionnelles (privées, politiques, liées à une seconde activité professionnelle,...), il semble que c'est bien le travailleur qui aura la qualité de responsable de traitement puisqu'il traite des données à d'autres fins que celles mises en oeuvre par l'employeur et qu'il a lui-mêmes déterminées.

Il n'est pas toujours aisé de déterminer si un usage de courrier électronique se situe dans le cadre des activités strictement professionnelles ou s'il relève d'une autre activité. Ainsi, si l'on conçoit que l'échange de correspondance électronique entre travailleurs s'inscrit dans un contexte professionnel, il n'est pas exclu qu'il ne relève pas de l'exercice de tâches professionnelles mais plutôt d'échanges à titre privé. Dans ce cas, ils ne relèvent pas des traitements mis en oeuvre par l'employeur.

L'identification du responsable du traitement n'est pas anodine car elle sera déterminante en matière de responsabilité en cas de violation de la législation de la protection des données. Cette problématique nous permet également de mettre en perspective la situation particulière de l'employeur responsable de traitement : alors qu'il est tenu en vertu de l'article 6 § 2 de la directive 95/46/CE de faire respecter la législation relative à la protection de la vie privée par ses travailleurs, il ne peut néanmoins s'affranchir des principes définis par cette législation lorsqu'il contrôle l'usage qui est fait du courrier électronique.

III.2. LE CONTRÔLE EN TANT QUE TRAITEMENT DE DONNÉES À CARACTÈRE PERSONNEL

Les opérations de contrôle ou de surveillance de l'utilisation des outils que sont le courrier électronique, l'Internet ou le téléphone seront mises en œuvre au travers de traitements dès qu'ils impliquent, ne serait-ce que partiellement, l'utilisation de moyens automatisés, ce qui est généralement le cas. Encore faut-il, pour qu'ils tombent dans le champ d'application de la directive, que ces traitements portent sur des données à caractère personnel.

De l'avis du Groupe de l'article 29, la surveillance de l'accès à Internet ou au courrier électronique du travailleur implique bel et bien un traitement de données à caractère personnel. Par contre, le contrôle de l'accès à l'Internet n'impliquerait pas forcément de traitement de données à caractère personnel. Tel est le cas lorsque le contrôle est ef-

fectué à un niveau si élevé qu'il ne permet pas de lier une personne en particulier à l'accès à certains sites ou modes d'accès ou si seules des données agrégées sont produites (8).

Dans la mesure où le contrôle de l'usage du courrier électronique, de l'Internet ou du téléphone constituera effectivement un traitement de données à caractère personnel, il devra être conforme aux principes définis par la directive 95/46/CE. Nous épinglerons à cet égard six grands principes traduisant les exigences les plus essentielles de cette directive en ce qui concerne l'admissibilité du traitement.

III.2.1. Principe de licéité

Aux termes de l'article 6, 1, a), le traitement doit être licite. L'exigence de licéité implique que le contrôle ne peut enfreindre une disposition de droit interne, par exemple assurant la confidentialité des communications électroniques ou des règles particulières en matière de données relatives aux trafic. Nous reviendrons sur cette problématique sous le chapitre IV.

III.2.2. Principe de transparence

L'article 6, 1, a) de la directive exige également que le traitement soit loyal. Le principe de loyauté se traduit essentiellement par l'obligation d'information que l'on retrouve définie aux articles 10 et 11 de la directive 95/46/CE. Le contrôle ne peut donc être secret mais doit, au contraire, faire l'objet d'une information préalable destinée aux travailleurs. Ainsi, le Groupe de l'article 29 estime-t-il qu'un employeur pourrait avoir un intérêt légitime à contrôler les performances de ses travailleurs en évaluant leurs prestations à l'aide d'ordinateurs (par exemple, surveiller le temps qu'un travailleur a passé à dactylographier, le nombre de fichiers enregistrés, l'heure à laquelle il a allumé et éteint son ordinateur, etc.) pour autant que les travailleurs en aient été informés. Par contre, si cette surveillance a été réalisée à l'insu du personnel, le traitement des données des travailleurs est en contradiction avec les dispositions de la directive 95/46/CE (9).

Concrètement, cette exigence de transparence ne semble pas requérir une information ad hoc lors de chaque contrôle effectué mais pourrait se traduire par une information générale et préalable communiquée aux travailleurs. C'est d'ailleurs l'avis du Groupe de l'article 29 qui précise que l'obligation de transparence dans ce contexte se traduit par une obligation de fournir à son personnel une déclaration

(8) Avis 8/2001, *op.cit.*, p.14.

(9) Avis 8/2001, *op.cit.*, p. 27.

claire, précise et aisément accessible de sa politique relative à la surveillance du courrier électronique et de l'utilisation de l'Internet (10).

Le contenu de l'information doit être conforme aux exigences de l'article 10 de la directive 95/46/CE et, tout en avisant de la possibilité des contrôles effectués par l'employeur, il doit préciser leurs finalités ainsi que fournir toute autre information qui s'avère nécessaire pour assurer la loyauté du traitement. Dans ce cadre, il pourrait être exigé d'informer les travailleurs sur les circonstances, modalités et portée du contrôle ou de la surveillance et identifier les personnes chargées de les effectuer par référence à leur fonction par exemple ainsi que les personnes susceptibles de recevoir communication de ces informations.

Le Groupe de l'article 29 recommande quant à lui la communication des informations suivantes (11) :

- les lignes directrices de l'entreprise concernant l'utilisation du courrier électronique décrivant dans le détail dans quelle mesure les systèmes de communication de l'entreprise peuvent être utilisés à des fins privées ou personnelles par les salariés (par exemple les limites concernant les périodes et la durée d'utilisation) ; concernant l'usage du courrier électronique, le Groupe de l'article 29 recommande également que l'employeur indique si le travailleur est ou non autorisé à disposer d'un compte de courrier électronique à usage strictement personnel, si l'utilisation de comptes de messagerie web est autorisée sur le lieu de travail et si l'employeur recommande à son personnel l'utilisation d'un compte privé de messagerie web pour utiliser le courrier électronique à des fins strictement personnelles. En ce qui concerne la consultation de l'Internet, le Groupe de l'article 29 invite les employeurs à préciser si, le cas échéant, certains éléments ne peuvent être visualisés ou copiés ;
- les motifs et les finalités de l'éventuelle mise en place d'une surveillance ;
- des informations détaillées sur les mesures de surveillance prises (qui surveille, quand et comment) ; quant à l'usage de l'Internet, le Groupe de l'article 29 considère que les travailleurs doivent être informés des systèmes installés pour empêcher l'accès à certains sites ou pour détecter une éventuelle utilisation abusive ;

(10) Document de travail du Groupe de l'article 29 concernant la surveillance des communications électroniques sur le lieu du travail adopté le 29 mai 2002, 5401/01, WP 55, pp.14 et 15.

(11) Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, pp. 15, 22 et 25.

- des informations détaillées sur les procédures d'application précisant comment et quand les travailleurs seront avertis en cas d'infraction aux lignes directrices internes et pourront réagir dans un tel cas. Le Groupe de l'article 29 recommande que l'employeur informe immédiatement le travailleur d'un quelconque abus des communications électroniques détecté, sauf si des raisons impérieuses justifient la poursuite de la surveillance ;
- la durée de conservation des éventuelles copies de sauvegarde des messages et le moment où les messages électroniques sont définitivement effacés du serveur ;
- les mesures de sécurité en place. ;
- l'implication éventuelle des représentants des travailleurs dans la mise en place de la politique de contrôle et de surveillance.

Une autre manière, en effet, de mettre en œuvre ce principe de transparence est de soumettre aux représentants des travailleurs la politique de contrôle que l'employeur entend mettre en place. Cette communication et discussion préalables des organisations représentatives des travailleurs peuvent d'ailleurs s'avérer obligatoires en exécution de la directive 2002/14/CE relative à la consultation des travailleurs (12) qui prévoit une obligation d'informer et de consulter les salariés concernant les décisions susceptibles d'entraîner des changements importants dans l'organisation du travail. La Commission envisage d'ailleurs d'intégrer dans une proposition de directive une obligation d'information et de consultation des représentants des travailleurs avant l'introduction, la modification ou l'évaluation de tout système susceptible d'être utilisé à des fins de surveillance ou de contrôle (13).

Soulignons que ce principe d'information préalable ne va pas toutefois pas sans soulever quelque opposition. Il ressort tant des besoins exprimés par les partenaires sociaux consultés que des considérations du Groupe de l'article 29 qu'une surveillance secrète devrait, dans certaines circonstances être admise (14). Ainsi la Commission envisage-t-elle de permettre une surveillance secrète en cas de soupçon raisonnable d'une activité criminelle ou d'un autre acte répréhensible dans le

(12) Directive 2002/14/CE du Parlement européen et du Conseil du 11 mars 2002 établissant un cadre général relatif à l'information et la consultation des travailleurs dans la Communauté européenne.

(13) « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *.op.cit.*, p. 19.

(14) Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, p. 15.

chef d'un travailleur (15). Or l'article 10 ne prévoit pas d'exception sur laquelle pourrait se fonder l'employeur pour effectuer une surveillance secrète. Les États membres ont néanmoins la possibilité, en vertu de l'article 13, g) de la directive, de prendre des mesures législatives visant à limiter la portée des obligations prévues à l'article 10 lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la protection des droits et libertés d'autrui. Il ne nous paraît cependant pas nécessaire de permettre un contrôle secret. En effet, à partir du moment où l'on admet que l'obligation d'information peut être accomplie par la communication d'une information préalable adressée à tous les employés, il est parfaitement envisageable d'y décrire les modalités de contrôle qui seront appliquées dans le cadre d'un soupçon d'une activité criminelle dans le chef d'un travailleur.

III.2.3. Principe de finalité

Les données collectées à des fins de contrôle devront en outre toujours l'être pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, comme stipulé par l'article 6,1, b de la directive 95/46/CE.

Cette exigence requiert, selon nous, que l'employeur ne se contente pas de considérer le contrôle comme une finalité en soi mais qu'il détermine les finalités du contrôle ou de la surveillance de façon suffisamment précise (par exemple, contrôle du bon fonctionnement du réseau ou contrôle du respect des directives de l'entreprise concernant l'utilisation du courrier électronique).

Le principe d'interdiction de réutilisation des données implique également que ce n'est pas parce qu'un employeur collecte et conserve des informations pour une finalité de contrôle particulière qu'il peut réutiliser ces informations dans le cadre d'un autre type de contrôle. La Commission et le Groupe de l'article 29 citent l'exemple suivant : les données collectées afin d'assurer la sécurité, le contrôle ou le bon fonctionnement des systèmes de traitement ne devraient pas être traitées dans le but de contrôler le comportement de chaque travailleur (16).

(15) « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op.cit.*, p. 19.

(16) Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, p.14 ; « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op.cit.*, p. 19.

III.2.4. Principe de nécessité

Le contrôle ou la surveillance de l'usage du courrier électronique ou d'autres moyens mis à la disposition du travailleur doit être nécessaire pour réaliser la finalité fixée. Ainsi, l'employeur devrait-il toujours se poser la question préalable de savoir s'il ne peut atteindre ses objectifs par d'autres moyens de supervisions moins intrusifs.

Ainsi le Groupe de l'article 29 considère-t-il par exemple que l'employeur devrait privilégier la prévention plutôt que la détection en ce qui concerne l'utilisation de l'Internet en ayant recours, dans la mesure du possible, à des outils techniques verrouillant l'accès à certains sites ou générant des avertissements automatiques (17).

III.2.5. Principe de légitimité

Les finalités de traitement devront en outre être légitimes, c'est-à-dire ne pas porter une atteinte disproportionnée aux intérêts de la personne concernée par rapport à l'intérêt que l'employeur peut trouver à contrôler son travailleur. Le respect de cette condition de proportionnalité appelle donc un équilibre et est sujette à appréciation. Le législateur européen a néanmoins d'ores et déjà déterminé à l'article 7 de la directive 95/46/CE les sept hypothèses dans lesquelles un traitement de données à caractère personnel poursuit *a priori* une finalité légitime. L'employeur ne pourra effectuer de contrôle ou de surveillance que dans la mesure où il peut justifier de l'une de ces bases de légitimité telles que transposées dans la loi nationale applicable.

Parmi celles-ci, on en retrouve plusieurs qui peuvent a priori offrir une base intéressante à l'employeur : le consentement du travailleur, l'exécution d'un contrat, l'obligation légale et le dernier cas prévu par la directive et reprenant l'existence d'une balance d'intérêt entre intérêt de la personne concernée et intérêt du responsable du traitement.

En ce qui concerne le consentement du travailleur, on constatera d'emblée les limites offertes par cette hypothèse. En effet, ce cas de figure ne peut offrir une base de traitement que lorsque seules les données du travailleur sont concernées. Tel ne sera pas le cas de l'utilisation du courrier électronique impliquant un expéditeur ou un destinataire externe dont on n'aura pas obtenu le consentement. De plus, la valeur d'un consentement donné par un travailleur dans le contexte de la relation de travail est mise en cause. Aux termes de l'article 2, h) de la directive 95/46/CE, le « consentement de la personne concernée» implique une manifestation de volonté, libre, spéci-

(17) Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, p. 24.

fique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement. Peut-on considérer que le consentement d'un travailleur est libre lorsqu'il est requis dans le cadre d'une relation d'autorité ? La Commission semble en douter et considère que l'employeur devrait éviter de recourir exclusivement au consentement pour légitimer un traitement de données à caractère personnel et devrait pouvoir se fonder sur d'autres motifs légitimes »(18).

On pourrait également penser à l'hypothèse de l'exécution du contrat de travail pour justifier le contrôle ou la surveillance d'un travailleur. Cependant, l'article 7, b) de la directive exige que le traitement soit nécessaire à l'exécution du contrat. Cette base ne nous paraît être pertinente que dans les cas particuliers où l'exécution du contrat de travail implique ou exige effectivement qu'un contrôle ou une surveillance soit exécutée de l'utilisation des outils de communication électronique, de par la nature même des prestations à effectuer. La seule existence de l'autorité de l'employeur sur ses travailleurs conférant au premier un pouvoir de contrôle et de surveillance de la bonne exécution des prestations de travail par les seconds ne semble en effet pas impliquer pour autant l'existence d'une nécessité d'effectuer un contrôle de l'usage des courriers électroniques, de l'Internet ou du téléphone pour assurer cette surveillance.

Si le critère de la nécessité du respect d'une obligation légale à laquelle le responsable du traitement est soumis peut offrir ponctuellement une base pour effectuer un traitement, l'employeur devra bien souvent se rabattre sur le critère de l'article 7, f. Celui-ci requiert que le traitement soit nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

Le bénéfice de cette base de justification appelle donc une balance d'intérêts qui doit être effectuée au cas par cas. À titre d'exemple, parmi les finalités de contrôle envisagées par la Commission, se retrouvent le contrôle destiné à vérifier ou à assurer le bon fonctionne-

(18) « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op.cit.*, pp. 12 et 13. Le Groupe de l'article 29 considère quant à lui que dans le cadre d'un contrôle du travailleur, si le consentement du travailleur peut entrer en ligne de compte pour déterminer si le traitement satisfait à l'article 6 de la directive, il ne peut jamais être le facteur déterminant de la légitimité (avis 8/2001, *op.cit.*, p. 24).

ment du système, pour des raisons de santé ou de sûreté ou encore en cas d'activité criminelle ou manquement grave d'un travailleur (19).

Le critère n'offre pas de certitude ni aux employeurs ni aux travailleurs sur la légitimité des finalités de contrôle. On pourrait dès lors envisager de définir comme acceptables certaines finalités de contrôle susceptibles d'être mises en oeuvre par un employeur ce qui revient à effectuer ce travail de mise en balance des intérêts en lieu et place des parties concernées (20). La Commission va même plus loin : elle estime qu'une obligation de soumettre toute politique de surveillance ou de contrôle à un examen préalable de l'autorité nationale chargée de surveiller la protection des données devrait être envisagée (21).

III.2.6. Principe de proportionnalité

Aux termes de l'article 6, 1, c de la directive 95/46/CE, les données collectées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement. Ce principe conduit à limiter les données qui peuvent être collectées et traitées de différentes manières.

Tout d'abord, on aura égard aux modalités de contrôle admissibles au regard des finalités poursuivies. Ainsi le Groupe de l'article 29 considère-t-il que si des employeurs pouvaient être autorisés à contrôler les données relatives au trafic, ils ne pourraient certainement pas en principe accéder au contenu des communications électroniques de leurs travailleurs (22). Il estime également qu'une utilisation abusive de l'Internet peut dans bien des cas être établie sans examiner le

---

(19)« Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op.cit.*, p. 19.

(20) Par exemple, la Convention collective de travail n°81 rendue obligatoire par le législateur belge prévoit qu'un contrôle ne peut être effectué que pour certaines finalités de contrôle à savoir :

1° la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;

2° la protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires ;

3° la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise ;

4° le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.

(21) « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op.cit.*, 19.

(22) Avis 8/2001, *op.cit.*, p. 34 ; Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, p.14.

contenu des sites consultés (23). Il est cependant indéniable que dans certaines hypothèses, il est impossible de réaliser le but poursuivi sans prendre connaissance du contenu d'une communication ou que l'absence de prise de connaissance du contenu pourrait obliger l'employeur à se contenter de simples suspicions. Ainsi la prévention de certains comportements illicites tels que la diffamation ou encore la communication d'images pédophiles ne pourra être assurée efficacement sans la possibilité de prendre connaissance du contenu des communications suspectes.

Une autre implication de ce principe de proportionnalité s'exprime dans l'admission ou non du caractère continu du contrôle et de la surveillance. La collecte continue d'informations sur le trafic des courriers électroniques sera plus aisément admissible à des fins de bonne administration et protection du réseau, que pour s'assurer que les travailleurs ne commettent pas d'actes répréhensibles, finalité dont on estime qu'elle n'appelle qu'un contrôle ponctuel. La Commission suggère de n'autoriser la surveillance continue que pour des raisons de santé, de sécurité, de sûreté ou de protection des biens de l'entreprise (24).

Le principe prévaut également en ce qui concerne les contrôles collectifs et individualisés : le caractère général ou individualisé des contrôles doit être justifié au vu de la finalité poursuivie. La Commission note que : « sauf dans certains cas, par exemple dans le cadre d'une surveillance automatisée visant à assurer la sécurité et le bon fonctionnement du système (par exemple, pour le protéger contre les virus), la surveillance systématique de l'utilisation du courrier électronique ou d'Internet par chaque travailleur devrait être interdite. Une surveillance individuelle pourrait être effectuée lorsqu'une activité criminelle, un acte répréhensible ou un manquement grave (25) peut raisonnablement (26) être soupçonné(e), à condition qu'il n'existe aucun autre moyen moins indiscret d'atteindre le résultat souhaité (par exemple, la surveillance objective du trafic de données plutôt que du contenu des messages électroniques, l'utilisation préventive de la technologie, etc.) »

Dans un même ordre d'idées, les données ne pourront être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation

(23) Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, p. 24.

(24) « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op.cit.*, p. 19.

(25) Souligné par l'auteur.

(26) Souligné par l'auteur.

des finalités de contrôle pour lesquelles elles sont collectées comme exigé à l'article 7,1,e.

III.3. Le contrôle et les données sensibles

Il n'est pas exclu que le contrôle exercé implique le traitement de données à caractère personnel dites « sensibles ». Il s'agit de données qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données relatives à la santé et à la vie sexuelle ainsi que les données judiciaires (27). Il en serait par exemple ainsi du contenu de courriers électroniques interceptés concernant l'appartenance politique ou syndicale du travailleur. Le traitement de ces données est en principe interdit en vertu de l'article 8 de la directive. Le traitement n'est autorisé que dans le cadre d'exceptions prévues dans les législations nationales.

Ce traitement soulève dès lors une première difficulté: l'employeur doit pouvoir se prévaloir d'une des hypothèses prévues dans la directive et transposée dans la législation nationale applicable. Parmi celles reprises dans la directive, trois nous semblent plus pertinentes en ce concerne le cas du contrôle exercé par l'employeur sur ses travailleurs.

Tout d'abord le traitement est possible avec le consentement des personnes concernées. Toutefois, comme nous l'avons signalé ci-avant, la possibilité d'un consentement libre dans le cadre d'une relation de travail est fortement mise en cause. Par ailleurs, dès que la communication concerne une personne externe à l'entreprise, il devient illusoire de vouloir obtenir son consentement.

La directive prévoit également la possibilité de traiter des données sensibles lorsque le traitement est nécessaire aux fins de respecter les obligations et les droits spécifiques du responsable du traitement en matière de droit du travail, dans la mesure où il est autorisé par une législation nationale prévoyant des garanties adéquates. L'applicabilité de cette exception exige donc que l'employeur soit autorisé ou tenu d'effectuer le traitement des données sensibles dans le cadre de son activité de contrôle des travailleurs, ce qui nous semble peu probable. La directive indique cependant par ailleurs que les États membres peuvent prévoir, pour un motif d'intérêt public important, des dérogations autres que celles prévues par la directive soit par leur législation nationale, soit sur décision de l'autorité de contrôle.

(27) C'est-à-dire les données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ainsi que les données relatives aux sanctions administratives ou aux jugements civils.

Une seconde difficulté inhérente à cette problématique est que l'employeur bien souvent ignore quel type de données le contrôle et/ou la surveillance effectuée peut l'amener à collecter. Cela signifie que dans nombre de cas l'employeur ne pourra déterminer à l'avance qu'il ne collectera et ne traitera que des données non sensibles et que le caractère sensible ou non des données obtenues ne sera révélé qu'au cours du contrôle effectué. Il en résulte que si l'employeur peut se prévaloir d'une des causes de justification prévue à l'article 7 de la directive pour le traitement des données non sensibles mais non d'une exception lui permettant de traiter des données sensibles, il se trouve face à un problème pratique difficilement surmontable.

Cette même impossibilité d'effectuer une sélection préalable des données traitées dans le cadre d'un contrôle entraîne une autre conséquence: le régime le plus strict devrait s'appliquer au traitement de toutes les données. Ainsi la possibilité d'être amené à prendre connaissance de données relatives à la santé oblige l'employeur à respecter les garanties posées par la législation nationale pour traiter ce type de données, par exemple la supervision du traitement par un praticien de la santé. Tout en reconnaissant le problème, le Groupe de l'article 29 plaide pour le simple fait que le traitement qui pourrait impliquer inévitablement certaines données sensibles n'empêche ou ne complique sérieusement les activités de surveillance par ailleurs légitimes (28).

Ces difficultés impliquent selon nous la plus grande prudence dans la manière dont les contrôles sont mis en œuvre et plaident également pour l'adoption de moyens de contrôle collectant le minimum de données.

IV. RÈGLES ÉMANANT DE LA DIRECTIVE 2002/58/CE

Comme exposé sous le point III, le contrôle effectué par l'employeur sur l'utilisation du courrier électronique, de l'Internet et du téléphone qui constitue un traitement de données à caractère personnel est soumis aux principes de la directive 95/46/CE. L'une des conditions du traitement est que ce dernier soit licite et respecte donc les autres régulations éventuellement applicables, tel l'article 5 §§1 et 2 de la directive 2002/58/CE relatif au secret des communications électroniques.

Les dispositions de la directive 2002/58/CE protègent des abonnés et utilisateurs indépendamment du contexte dans lequel il est fait usage des services de communications électroniques ou de réseaux de

(28) Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.* p. 17.

communications électroniques. En particulier, le secret des communications est garanti également dans le contexte de la relation de travail.

La directive 2002/58/CE constitue, en outre, une réglementation spécifique qui complète la directive 95/46/CE pour ce qui concerne les traitements effectués dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans la Communauté. Il y a lieu également de tenir compte de certains aspects relatifs à la réglementation du traitement des données relatives au trafic dans la mesure où elle peut inférer sur les données que l'employeur peut être amené à se procurer concernant les données de communications électroniques de ces travailleurs.

IV.1. PRINCIPE DE L'INTERDICTION DE LA SURVEILLANCE ET DE L'INTERCEPTION DE COMMUNICATIONS ÉLECTRONIQUES

Le premier paragraphe de l'article 5 de la directive 2002/58/CE prévoit que « les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée conformément à l'article 15, paragraphe 1» (29). Il a cependant immédiatement précisé que « le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité ».

IV.1.1. Portée du paragraphe 1 de l'article 5

Il est intéressant de se pencher sur la question de la portée exacte de cette disposition et ce tant au regard des informations protégées, que

(29) En vertu duquel « *Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE* ».

des traitements pris en considération et du cadre technique de ces traitements.

IV.1.1.1. Les informations protégées

L'article 5 §1 porte à la fois sur les communications et sur les données relatives au trafic y afférentes. Qu'entend-on par ces termes ?

L'article 1(d) de la directive indique qu'une « communication » est « toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques (30) accessible au public » tout en précisant que « cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit ».

Une communication est donc, aux termes de la directive, l'information transmise au moyen du service de communications électroniques. Il s'agit tant de l'information transmise par courriers électroniques, communications téléphoniques (sur un réseau téléphonie fixe et mobile) que via l'Internet. Cette information est par ailleurs distincte des données relatives au trafic c'est-à-dire les données de transmission. Les données relatives au trafic sont en effet définies comme étant les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation (article 1 (b) de la directive 2002/58/CE).

Cette distinction se déduit à la fois du texte du paragraphe 1 de l'article 5 qui envisage une protection pour ces deux types d'information et de celui du considérant 15 de la directive. Ce dernier précise, en effet, qu'« une communication peut inclure toute information consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication ». Il les distingue, par ailleurs, des données relatives au trafic qui « peuvent, entre autres, comporter des données concernant le routage, la durée, le moment ou le volume d'une communication, le protocole de référence,

(30) Les services de communications électroniques sont définis comme suit : « *le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus ; il ne comprend pas les services de la société de l'information tels que définis à l'article 1^er de la directive 98/34/CE qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques* ». (directive 2002/21/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques, article 2 (c)).

l'emplacement des équipements terminaux de l'expéditeur ou du destinataire, le réseau de départ ou d'arrivée de la communication, ou encore le début, la fin ou la durée d'une connexion. Elles peuvent également représenter le format dans lequel la communication a été acheminée par le réseau ». Constituent par exemple des données relatives au trafic le numéro de téléphone de l'appelant et de l'appelé, le temps d'appel, l'adresse de courrier électronique, l'heure d'envoi, la taille du courrier électronique et l'adresse IP.

Bien que l'on puisse s'étonner de ce que dans une directive qui vise en principe à réglementer le traitement de données à caractère personnel dans une activité de transmission, on s'intéresse à la protection du contenu des communications, il résulte de ce qui précède que l'article 5 §1 protège tant l'information qui fait l'objet de la communication (le contenu de la communication) que les données relatives à la transmission de la communication.

IV.1.1.2. Les traitements pris en considération

Le paragraphe 5.1 vise expressément l'écoute, l'interception, le stockage ou la soumission à tout autre moyen d'interception ou de surveillance des communications et des données relatives au trafic y afférentes. En effet, dans le cadre d'une réglementation technique s'adressant à la transmission d'informations sur des réseaux de communications, il est logique de vouloir protéger l'information transmise et les données de communications contre une interception ou surveillance exécutée à l'insu des participants à la communication. Notons d'ailleurs que sur ce point la directive va plus loin qu'une imposition de telles restrictions aux fournisseurs des services ou des réseaux de communications électroniques qui sont généralement les destinataires des autres dispositions de la directive. Elle exige des États membres qu'ils assurent une protection contre de tels agissements dans le chef de tout tiers.

Tous les traitements expressément mentionnés font donc penser à une activité de surveillance ou d'interception à l'insu d'un ou de tous les participants à la communication au cours du processus de transmission et non à la prise de connaissance d'information a posteriori. Pourtant la première phrase de cet article permet le doute : elle exige la protection de la confidentialité de communications et des données relatives au trafic y relatives, les opérations visées dans la suite de l'article n'étant citées qu'à titre d'un minimum. Le texte invite donc les États membres à consacrer une protection des données relatives au trafic et/ou du contenu même après la transmission.

IV.1.1.3. Cadre technique

En ce qui concerne le cadre technique de l'article 5, il convient d'épingler son champ d'application limité. En effet, sont seuls concernés les réseaux qui sont utilisés entièrement ou principalement pour la fourniture de services de communications accessibles au public (31). Le traitement de données à caractère personnel effectué dans le cadre de réseaux fermés ou privés d'une entreprise relève uniquement de la directive 95/46/CE. La directive ne couvre donc pas le traitement de données à caractère personnel dans le contexte d'un intranet d'une entreprise mais bien la communication de données via l'Internet (32). Le Groupe de l'article 29 a d'ailleurs regretté cette limitation du champ d'application en relevant que « les réseaux privés revêtent une importance croissante dans la vie de tous les jours et les communications des citoyens, par exemple dans le cadre de leur travail, et les risques que de tels réseaux font courir à la vie privée augmentent en conséquence et deviennent plus spécifiques (par exemple surveillance du comportement des salariés au moyen de données relatives au trafic, absence de confidentialité des communications) » (33).

Cette restriction du champ d'application de la directive implique que, dès lors que la communication est effectuée au moyen d'un réseau privé, non seulement le principe de confidentialité de l'article 5 de la directive 2002/58/CE mais également les autres dispositions de la directive 2002/58/CE, notamment en ce qui concerne le traitement des données relatives au trafic ne s'appliquent pas (34). L'article 6 de la directive prévoit en effet dans le prolongement de l'article 5 que les données relatives au trafic doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sauf exceptions prévues au sein de cet article (pour la facturation, le marketing des services du fournisseur de services ou de réseau, la fourniture de services à valeur ajoutée,...) et soumises au respect de conditions particulières. Le fait que les articles 5 et 6 de la directive 2002/58/CE ne s'appliquent qu'aux traitements de données effectués sur des réseaux publics facilite donc grandement le traitement de données relatives au trafic ainsi que le contenu des communications effec-

(31) Directive 2002/21/CE, article 1(d).

(32) Y. POULLET, S. LOUVEAUX et M. V. PEREZ ASINARI, « Data Protection and Privacy in Global Networks : An European Approach.... », *The EDI Law Review*, 2001, p.152.

(33) Avis 7/2000 du 2 novembre 2000 sur la proposition, présentée par la Commission, de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques du 12 juillet 2000 (COM (2000) 385), p. 3.

(34) W. MAXWELL, « The communication data protection directive », in *Electronic communications: the new EU framework*, New York, Oceana Publications, décembre 2002, p. 1.5-6.

tuées sur des réseaux privés. Ceux-ci ne sont plus soumis qu'à la directive 95/46/CE.

Il existe donc une dualité de régimes qui pourra le cas échéant concerner une même entreprise. L'article 5 §1 devra être pris en compte pour certains contrôles lorsqu'il s'agit de communications réalisées via un réseau accessible au public tandis que d'autres relatifs à des communications échangées via un réseau privé ou fermé ne devront tenir compte que de la directive 95/46/CE.

IV.1.2. Principe

Le principe posé par l'article 5§1 est donc au minimum l'interdiction à toute personne autre que l'utilisateur d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance sans le consentement des utilisateurs concernés parties à la communication. La formulation générale de ce principe invite à sa pleine application dans le contexte de la relation entre un travailleur et un employeur, et ce tant en ce qui concerne des communications professionnelles que des communications privées.

Toute activité correspondant à celles décrites au sein de cette disposition requiert non seulement le consentement du travailleur partie à la communication (en tant qu'expéditeur ou destinataire d'un courrier électronique, auteur de communication téléphonique ou internaute) mais également de toute autre personne impliquée. Or si, on l'a vu, la possibilité d'obtenir un consentement libre de toute pression dans le chef du travailleur pose déjà question, il est quasiment impossible en pratique d'obtenir celui de personnes extérieures à l'entreprise. Il est intéressant de noter cependant que la directive 2002/58/CE exige le consentement des utilisateurs et pas nécessairement de toutes les personnes concernées par la communication, telles celles visées dans le contenu de celle-ci.

La directive ne laisse la possibilité aux États membres de déroger à cette exigence que par une loi prise en conformité avec l'article 15 de la directive. Cette disposition ne vise que des hypothèses limitées c'est-à-dire la sauvegarde de la sécurité nationale, la défense et la sécurité publique, ou la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques. Elle n'offre donc pas de marge de manœuvre aux États membres pour déroger à l'exigence du consentement préalable dans le contexte de la surveillance et du contrôle de l'usage d'outils informatiques dans le cadre d'une relation de travail, à moins que cela ne puisse s'inscrire dans le cadre des finalités de pré-

vention d'infractions pénales ou de prévention d'utilisation non autorisée de système de communications électronique. L'article 5 §1 laisse cependant une certaine marge de manœuvre aux États membres sur les opérations qui seront visées par la loi nationale. Les opérations visées pourront être variables d'un État à l'autre.

Le second paragraphe de l'article 5 de la directive 2002/58/CE prévoit toutefois la possibilité pour les États membres de permettre l'enregistrement de communications et des données relatives y afférentes dans d'autres hypothèses que celles visées par l'article 15 de la directive.

En effet, ce paragraphe 2 précise que « le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale ». Les États membres ont donc la possibilité d'autoriser l'enregistrement de communication et de données relatives au trafic y afférentes pour une finalité précise : la fourniture de la preuve d'une transaction commerciale ou d'une communication professionnelle.

Cette disposition pourrait permettre de résoudre la situation en permettant un retour de l'employeur à plus de maîtrise sur les communications à caractère strictement professionnel et en lui reconnaissant le droit de les enregistrer pour pouvoir attester plus tard de transactions commerciales ou de communications professionnelles intervenues. On peut toutefois s'interroger sur l'adéquation du terme « enregistrement » qui reste très restrictif sur le type d'opération autorisée (qu'en est-il de la prise de connaissance, de la communication à des tiers ?). Il nous semble en toute hypothèse que cette disposition n'envisage nullement le traitement de données à des fins de contrôle sur l'utilisation des moyens de communications par le travailleur.

IV.1.3. Conclusion

Cet article 5 §1 de la directive constitue donc un obstacle de taille à la surveillance ou au contrôle de l'employeur sur l'utilisation des outils de communications électroniques mis à la disposition de ses travailleurs dès que cela implique des opérations interdites sur un réseau de communications et de services de communications électroniques accessibles au public.

Il n'existe, en effet, pas *a priori* de possibilité offerte sous le couvert de la directive 2002/58/CE de prise de connaissance du contenu des communications électroniques ainsi que des données trafic y afférentes. On s'étonnera dès lors de trouver, dans un document de travail du

Groupe de l'article 29 du 29 mai 2002, une évocation d'une possibilité de prendre connaissance du contenu des communications moyennant information préalable des travailleurs et des personnes externes à l'entreprise qui communiquent avec les travailleurs (35).

Le Groupe semble fonder cette possibilité sur une vision plus nuancée du secret de la correspondance. Il considère que la notion de « correspondance » recouvre non seulement les lettres rédigées sur papier, mais aussi d'autres formes de communications électroniques reçues ou émises sur le lieu de travail, comme les appels téléphoniques émis ou reçus dans des locaux professionnels ou les messages électroniques reçus ou expédiés depuis les ordinateurs mis à disposition sur le lieu de travail (36). Il constate, par ailleurs, que le secret de la correspondance consacré par des textes internationaux notamment l'article 8 de la Convention européenne des droits de l'homme et l'article 7 de la Charte des droits fondamentaux de l'Union européenne connaît des principes et limites propres. Ainsi, le Groupe de l'article 29 déduit-il de la jurisprudence de la Cour européenne des droits de l'homme à propos de l'article 8 de la Convention dans le contexte professionnel notamment les principes suivant lesquels « les salariés peuvent légitimement s'attendre au respect de leur vie privée sur leur lieu de travail et ce droit n'est pas annulé par le fait qu'ils utilisent des outils de communication ou d'autres équipements professionnels de l'employeur » tout en concédant qu'« il semble néanmoins que la fourniture d'informations adéquates par l'employeur au salarié puisse diminuer la légitimité de cette attente » (37). Le Groupe de l'article 29 concède également qu'il existe une marge d'interprétation concernant les restrictions ou dérogations au principe du secret de la correspondance mis en balance avec d'autres droits ou libertés consacrés par la Convention européenne des droits de l'homme et que les législations des États membres peuvent différer à cet égard (38). Il

(35) Le Groupe de l'article 29 considère en effet que « *Si l'accès au contenu des messages est indispensable, il conviendrait de tenir compte du respect de la vie privée des destinataires externes comme des destinataires internes à l'organisation. Par exemple, l'employeur ne peut pas obtenir le consentement des personnes externes à l'organisation qui envoient des messages aux membres de son personnel. L'employeur doit mettre en oeuvre tous les moyens raisonnables pour avertir les personnes externes à l'organisation de l'existence d'activités de surveillance susceptibles de les affecter. On pourrait, par exemple, imaginer l'insertion d'avertissements sur l'existence de systèmes de surveillance dans tous les messages sortant de l'organisation* » (Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, p.18).

(36) Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, p.8.

(37) Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, p. 9.

(38) Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, p. 20.

semble dès lors considérer que l'employeur puisse dans certaines circonstances prendre connaissance du contenu d'une communication sans le consentement de toutes les parties à la communication (39), et ce nonobstant l'existence de l'article 5 §1 de la directive 97/66/CE remplacé depuis lors par l'article 5 §1 de la directive 2002/58/CE.

De son côté, la Commission prend quant à elle une position plus radicale que le principe de l'interdiction de prise de connaissance sans le consentement préalable dans le cadre des communications strictement privées des travailleurs. Elle considère opportun d'interdire cette prise de connaissance nonobstant le consentement du travailleur (40).

IV.2. ACCÈS AUX DONNÉES DE COMMUNICATIONS

Une autre façon d'envisager un contrôle de l'usage du courrier électronique, de l'Internet ou du téléphone est celui de l'accès à des données de communications par l'intermédiaire du fournisseur de ces services et de l'utilisation de ces données à des fins de contrôle. En effet, le fournisseur des services détient assurément des données permettant le cas échéant à un employeur de vérifier quel numéro de téléphone un travailleur a appelé ou éventuellement si une adresse IP peut être associée à un ou plusieurs travailleurs, sur quel site celui-ci ou l'un de ceux-ci s'est connecté. On constate toutefois que la directive entend tenir compte d'une particularité du secteur des communications : l'abonné du service n'est pas toujours la même personne que l'utilisateur.

La directive 2002/58/CE contient différentes dispositions qui régissent le traitement de telles données par les fournisseurs de services accessibles au public. Ainsi l'article 6 de la directive portant sur le traitement des données relatives au trafic pose comme principe que les données relatives au trafic ne peuvent être traitées par le fournisseur d'un service ou d'un réseau de communication électronique qu'afin d'assurer la transmission de la communication. Elles doivent être effacées ou rendues anonymes dès la finalité de transmission achevée. L'article 6 admet néanmoins quelques exceptions qui autorisent une conservation plus longue afin de mettre en œuvre des traitements sur ces données pour des finalités expressément autorisées par la directive.

Dès lors que des données relatives au trafic sont conservées pour y être traitées pour des finalités autorisées par la directive, on peut s'interroger sur le fait de savoir si un employeur pourra, en tant

(39) Document de travail concernant la surveillance des communications électroniques sur le lieu du travail, *op.cit.*, p. 18.

(40) « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », *op.cit.*, 19.

qu'abonné, demander à avoir accès aux données de ses travailleurs, utilisateurs du service. Ce problème se pose avec une acuité particulière en ce qui concerne l'usage d'un téléphone mobile attribué exclusivement par l'employeur à l'un de ses travailleurs. Tel pourrait être par exemple le cas pour certains programmes d'abonnement téléphonique mobile caractérisés par l'attribution de plusieurs numéros de téléphone ou lorsqu'il s'agit d'un abonnement à l'Internet….

On constate que l'article 6, s'il identifie les finalités pour lesquelles des données relatives au trafic peuvent être traitées ainsi que certaines conditions relatives au traitement, ne règle nullement le droit d'accès à ces données. Par contre, la directive aborde la question des données susceptibles d'être traitées et communiquées dans le cadre de la facturation d'un service.

L'article 6 § 2 précise, en effet, que les données qui sont nécessaires à la facturation peuvent être traitées à cette fin. Toutefois cette disposition n'identifie pas quelles données seront conservées et traitées dans le cadre de la mise en oeuvre de cette finalité ni celles qui seront le cas échéant communiquées d'office ou sur demande à l'abonné dans le cadre de la facturation de ses services. C'est l'article 7 de la directive qui traite de cette dernière problématique. Il précise tout d'abord que les abonnés ont le droit de recevoir des factures non détaillées. Il impose ensuite aux États membres de prendre des dispositions nationales afin de concilier les droits des abonnés recevant des factures détaillées avec le droit à la vie privée des utilisateurs appelants et des abonnés appelés, par exemple en veillant à ce que lesdits utilisateurs et abonnés disposent de modalités complémentaires suffisantes renforçant le respect de la vie privée pour les communications ou les paiements.

On constate donc que la directive est soucieuse de restreindre et les données traitées à des fins de facturation, et les données communiquées à l'abonné qui n'est pas l'utilisateur. Cela implique-t-il que cette disposition se substitue à celle de la directive 95/46/CE concernant le droit d'accès dans ce contexte particulier de traitements de données à caractère personnel ?

L'exercice du droit d'accès est en effet régi par l'article 12 de la directive 95/46/CE. Cette disposition prévoit que les États membres garantissent à toute personne concernée le droit d'obtenir du responsable du traitement notamment la confirmation que des données la concernant sont ou ne sont pas traitées, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données traitées et les destinataires ou les catégories de destinataires auxquels les données sont communiquées. Le titulaire du droit d'accès est donc la personne concernée par les données. Des termes de l'article 2

(a) de la directive, on ne peut comprendre la personne concernée que comme étant la personne physique identifiée ou identifiable sur laquelle portent les données à caractère personnel. Il s'agit donc dans le cas qui nous occupe de l'utilisateur. Le droit d'accès à des données à caractère personnel par une personne morale est également exclu.

En vertu du caractère complémentaire de la directive 2002/98/CE par rapport à la directive 95/46/CE, il faut se référer à cette dernière pour tout ce qui n'est pas réglé par la première. Comme mentionné supra, il est indéniable que la directive 2002/58/CE ne se penche pas explicitement sur le droit d'accès. Ce constat nous amène à penser que le droit d'accès n'est ouvert qu'à l'utilisateur du service et non à l'employeur.

Le contrôle de l'utilisation des outils tels que l'Internet ou le téléphone via l'obtention de données de la part de fournisseurs de services devrait donc être limité par la combinaison de l'application de l'article 7 de la directive 2002/58/CE et de l'article 12 de la directive 2002/58/CE. En toute hypothèse, si l'employeur devait entrer en possession de données à caractère personnel relatives à ses travailleurs par ce biais, il ne pourrait en faire un usage à des fins de contrôle que dans la mesure où il aurait respecté les principes issus de la directive 95/46/CE, notamment le principe de finalité.

V. CONCLUSION

L'application conjuguée des dispositions des directives 95/46/CE et 2002/58/CE érige de nombreuses limites voire même des obstacles au contrôle ou à la surveillance de l'usage du courrier électronique, de l'Internet ou du téléphone.

La plupart des principes définis dans la directive 95/46/CE ne posent pas de réelles difficultés d'application dans le contexte de ce contrôle ou de cette surveillance et l'encadrent d'ailleurs de façon appropriée. Le respect du principe de finalité et de nécessité nous semble par exemple tout à fait praticable tel quel. L'interdiction en principe de la surveillance ou du contrôle secret c'est-à-dire sans information préalable des travailleurs concernés nous paraît également appropriée même si certains acteurs du secteur, la Commission et le Groupe de l'article 29 semblent reconnaître qu'il est des cas où une surveillance ou un contrôle secret doivent pouvoir être exercés sous peine d'être inefficaces.

Par contre d'autres exigences de la directive posent de réelles difficultés d'application. Ainsi retiendra-t-on que le régime strict lié au traitement des données sensibles est difficile à prendre en compte dans

le cadre d'un contrôle dont l'employeur ne sait a priori quelles données il va révéler. Le principe de légitimité impose quant à lui à l'employeur de pouvoir justifier son contrôle à la lumière d'une des bases de légitimité admises par la directive. Dans bien des cas, seule la base de l'article 7, f sera applicable. Cette disposition appelle une mise en balance des intérêts en présence et donc une évaluation de la légitimité au cas par cas. Si cette base ouverte présente l'avantage de permettre une certaine souplesse, l'exercice de la mise en balance qu'elle suppose n'offre pas le confort de la certitude que les acteurs du secteur pourraient souhaiter. Nous retiendrons que ce constat est également transposable au respect de l'exigence de proportionnalité dans les moyens de contrôle utilisés et dans les données collectées par rapport à la finalité du contrôle. Ces incertitudes trouvent écho auprès de la Commission qui serait prête à définir des directives plus précises. Enfin, le principe de licéité est également source de difficultés. Il suffit de prendre en compte les dispositions de la directive 2002/58/CE pour s'en convaincre.

En effet, l'article 5 § 1 de la directive 2002/58/CE impose aux États membres d'assurer la confidentialité du contenu des communications électroniques effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public ainsi que des données relatives au trafic y afférentes. La directive ne permet a priori pas d'exceptions à ce principe de confidentialité dans le contexte d'un contrôle qu'un employeur effectuerait, légitimement par ailleurs, sur l'utilisation des moyens de communications électroniques. Ceci interdit donc ledit contrôle lorsqu'il implique la prise de connaissance ne serait-ce que de données relatives au trafic (telle l'identité du destinataire d'un courrier, les données de navigation sur Internet, le numéro appelé). La directive s'oppose *a fortiori* la consultation par l'employeur du contenu de la communication. La confidentialité s'applique tant aux communications professionnelles qu'à celles à caractère privé. Seules échappent à l'application de ce principe, les communications effectuées sur un réseau privé.

Si le principe de la confidentialité des communications électroniques semble tout à fait indiqué, même dans un contexte professionnel, son caractère absolu nous paraît moins justifiable. En effet, la légitimité même du principe d'un possible contrôle de l'utilisation des outils mis aux dispositions des travailleurs requiert que celui-ci puisse effectivement être mis en œuvre lorsqu'il respecte par ailleurs les principes posés par la directive 95/46/CE.

Ces considérations nous amènent à penser que l'application des directives 95/46/CE et 2002/58/CE dans le contexte du contrôle et de la surveillance de l'usage du courrier électronique, de l'Internet ou du

téléphone ne va pas sans difficultés et qu'un encadrement spécifique aurait toute sa pertinence.